磐田市立総合病院 情報セキュリティ対策基準

１ 目的

磐田市立総合病院情報セキュリティ対策基準（以下「本基準」という）は、磐田市情報セキュリティ基本方針のもと、磐田市立総合病院（以下「当院」という）における情報セキュリティ対策の具体的な遵守事項及び判断基準等を定めることを目的とする。

２ 定義

本基準で使用する定義は基本的には磐田市情報セキュリティポリシーの序章に定められたとおりとするが、以下の定義に関してはこれを優先して適用する。

(1) 情報システム

コンピュータ、ソフトウェア、ネットワーク及び記録媒体で構成され、医療情報及び行政情報を処理するための仕組みをいう。

(2) 職員等

当院の情報資産に接する職員、非常勤職員、臨時職員及び業務委託先の社員のうち当院で勤務するものをいう。

(3) 院内

当院の敷地内をいう。

(4) 事務局

経営企画課のことをいう。

(5) 通信経路の分割

医療情報システム系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

３ 適用範囲

(1) 組織

本基準が適用される組織は、当院の職員等により構成される。

(2) 情報資産

情報セキュリティ対策基準が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム及びこれらに関する設備、記録媒体

② 診療情報及び情報システム関連文書などの紙媒体及び電子媒体の情報

４ 組織体制

当院の情報資産について、適切に情報セキュリティ対策を実施するための体制を次に掲げるとおりとする。

(1) 情報セキュリティ統括責任者

① 情報資産の管理及び情報セキュリティ対策に関する最高責任者として、情報セキュリティ統括責任者を置く。

② 情報セキュリティ統括責任者は、病院長をもってこれに充てる。

(2) 情報セキュリティ副統括責任者

① 情報資産の管理及び情報セキュリティ対策に関する権限及び責任を有する者として、情報セキュリティ副統括責任者を置く。

② 情報セキュリティ副統括責任者は、情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
③ 情報セキュリティ副統括責任者は、情報セキュリティ統括責任者を補佐する。
④ 情報セキュリティ副統括責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報セキュリティ担当者に対して、情報セキュリティに関する指導及び助言を実施する。
⑤ 情報セキュリティ副統括責任者は、当院の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、情報セキュリティ統括責任者の指示に従い、情報セキュリティ統括責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。
⑥ 情報セキュリティ副統括責任者は、情報資産に関する情報セキュリティ実施手順の維持・管理を行う統括的な権限及び責任を有する。
⑦ 情報セキュリティ副統括責任者は、緊急時等の円滑な情報共有を図るため、情報セキュリティ統括責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報セキュリティ担当者を網羅する連絡体制を整備する。
⑧ 情報セキュリティ副統括責任者は、情報セキュリティ統括責任者が、副病院長の中から指名する。

(3) 情報セキュリティ責任者
① 各部等の情報セキュリティ対策に関する統括的な権限及び責任を有する者として、情報セキュリティ責任者を置く。
② 情報セキュリティ責任者は、その所管する部等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
③ 情報セキュリティ責任者は、その所管する部等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を実施する。
④ 情報セキュリティ責任者は、副病院長、理事及び各部長（地域医療支援センター長を含む。）をもってこれに充てる。

(4) 情報セキュリティ管理者
① 所管する部、科、課、室の情報セキュリティ対策に関する権限及び責任を有する者として、情報セキュリティ管理者を置く。
② 情報セキュリティ管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
③ 情報セキュリティ管理者は、その所管する部、科、課、室において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者、情報セキュリティ副統括責任者及び情報セキュリティ統括責任者へ速やかに報告を行い、指示を受ける。
④ 情報セキュリティ管理者は、各部、科、課、室長をもってこれに充てる。

(5) 情報セキュリティ担当者
各部、科、課、室において、情報セキュリティの実務を行う職員を情報セキュリティ担当者とし、情報セキュリティ管理者が指名する。

(6) 情報セキュリティ委員会
① 情報セキュリティに関する適正な運用及び管理を行うために、情報セキュリティ

委員会を設置する。

② 情報セキュリティ委員会は、情報セキュリティ統括責任者、情報セキュリティ副統括責任者、情報セキュリティ責任者及び事務部各課長をもって構成し、情報セキュリティポリシーの見直し、情報セキュリティ対策の実施及び実施状況の把握など情報セキュリティ対策に関する重要事項を審議する。

③ 情報セキュリティ委員会事務局を経営企画課に置く。

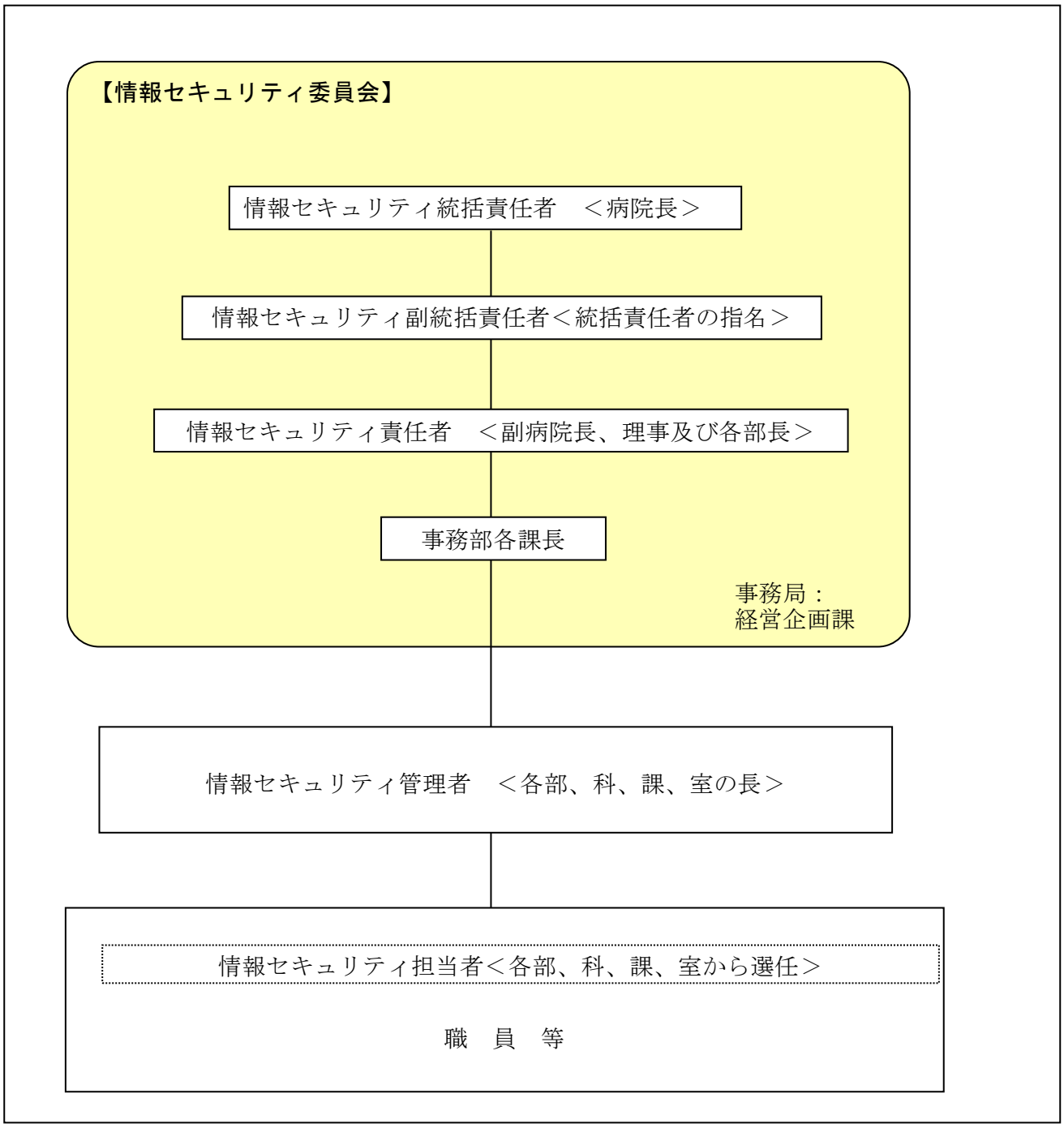

図１　情報セキュリティ組織体制図

5 情報資産の分類と管理方法

5.1 情報資産の分類

本院における情報資産は、次のとおり分類し、必要に応じ取り扱いを制限する。

表１　情報資産の分類

<table>
<tr><th>分類</th><th colspan="2">機密性</th><th colspan="2">完全性</th><th colspan="2">可用性</th></tr>
<tr><td rowspan="6">重要な情報資産</td><td>機密性３</td><td>情報が漏えいした場合に、個人に損失及び不利益を与える情報資産</td><td rowspan="2">完全性２</td><td rowspan="2">業務で取り扱う情報資産のうち、改ざん、書換え又は破損により、個人若しくは法人の権利が侵害される、又は業務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産</td><td rowspan="2">可用性２</td><td rowspan="2">業務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、個人若しくは法人の権利が侵害される、又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産</td></tr>
<tr><td>機密性２</td><td>情報が漏えいした場合に、業務の遂行に支障を与える情報資産</td></tr>
<tr><td>事　例</td><td colspan="5">・医療情報等で個人の重要なデータに関する項目を扱った文書やデータなど。
・個人情報の入った各種資料、重要な会議の議事録など
・上記に該当する重要な情報を含む情報システム及びシステム関連文書など
・その他、法令、規則等で使用が制限されている文書やデータなど</td></tr>
<tr><td>取り扱い</td><td colspan="5">・施錠管理
・堅牢なシステム管理
・履歴管理（推奨）</td></tr>
<tr><td>共有範囲</td><td colspan="5">・関係者のみ共有（情報収集の目的業務を実施管理する職員等を含む）</td></tr>
<tr><td>他者利用</td><td colspan="5">・業務上必要な場合において、必要な手続き及び承認を得た場合に利用可能</td></tr>
<tr><td rowspan="4">その他の情報資産</td><td>機密性１</td><td>機密性２又は機密性３以外の情報資産</td><td>完全性１</td><td>完全性２以外の情報資産</td><td>可用性１</td><td>可用性２以外の情報資産</td></tr>
<tr><td>取り扱い</td><td colspan="5">・データが破損しないレベルでの管理
・業務に影響の無い範囲で第三者への開示可能</td></tr>
<tr><td>共有範囲</td><td colspan="5">・院内共有</td></tr>
<tr><td>他者利用</td><td colspan="5">・業務上必要な範囲において利用可能</td></tr>
</table>

5.2 情報資産の管理

(1) 管理責任

① 情報セキュリティ管理者は、所管する情報資産について管理責任を有する。

② 情報セキュリティ管理者は、所管する情報資産のうち、「重要な情報資産」に関する情報資産台帳（様式１）を作成し、内容を適宜更新する。

③ 情報セキュリティ管理者は、情報資産台帳の内容について、職員に周知するとともに、安全な場所に管理し、適切に保管する。

④ 情報資産が複製又は伝送された場合には、複製等された情報資産も「表1 情報資産の分類」に基づき管理する。

⑤ 情報セキュリティ管理者は、作成・更新を行った情報資産台帳について、速やかにその写しを経営企画課に提出する。

(2) 情報の作成

① 職員等は、業務上必要のない情報を作成しない。

② 情報を作成する者は、「表1 情報資産の分類」に基づき、当該情報を取り扱う。

③ 情報を作成する者は、作成途上の情報についても、紛失や流出等を防止する。また、情報の作成途上で不要になった場合は、当該情報を消去する。

(3) 情報資産の入手

① 院内の情報資産を入手した場合は、入手元の情報資産の分類に基づき取り扱う。

② 院外の情報資産を入手した場合は、「表1 情報資産の分類」に基づき取り扱う。

③ 入手した情報資産の分類が不明な場合は、情報セキュリティ管理者の指示に従う。

(4) 情報資産の利用

① 職員等は、業務以外の目的に情報資産を利用しない。

② 情報資産を利用する者は、「表1 情報資産の分類」に基づき、適切な取り扱いをする。

③ 情報資産を利用する者は、記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って取り扱いをする。

(5) 情報資産の保管

① 情報セキュリティ管理者は、「表1 情報資産の分類」に基づき、情報資産を適切に保管する。

② 情報セキュリティ管理者は、情報資産を記録した記録媒体を長期保管する場合は、書込禁止の措置を講じる。

③ 情報セキュリティ管理者は、「重要な情報資産」を保管する場合、施錠可能な場所、もしくは堅牢なシステム管理下に保管する。

(6) 情報資産の持ち出し及び提供等

① 職員等は、「重要な情報資産」を外部に持ち出し及び提供を行う場合には、匿名化等の措置をして、個人が特定できない形にする。

(7) 情報資産の廃棄

① サーバやパソコン等の機器や記録媒体のデータ消去、廃棄、リース返却を行う場合は、情報セキュリティ管理者が経営企画課に申し出る。

② 「重要な情報資産」を記録した紙媒体を廃棄する場合は、機密書類扱いにて溶解処理または焼却処理をする。また廃棄まで施錠可能な場所に保管する。

③ 「重要な情報資産」を廃棄した場合、情報セキュリティ管理者は情報資産台帳を

更新する。

④ クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認する。なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

6 物理的セキュリティ

6.1 部署部門の管理

部署部門を所管する情報セキュリティ管理者は、以下の措置を講じる。

① 第三者の入室を制限すべき部署部門は、施錠管理を実施する。

② 部署部門に重要な情報資産を保管する場合には、部署部門の施錠の有無にかかわらず個別に施錠管理を実施する。その場合、外部からは存在がわからないような対策を実施する。

③ 施錠保管することにより、業務に支障のある重要な情報資産については、部署部門の入口から離れた場所に保管し、カバーをするなどして、その存在をできるだけ第三者にわからないような対策を実施する。

④ 画面が第三者に見られる可能性のあるところに設置されているパソコンには、プライバシーフィルターの使用、画面の向きの変更、パーティションの利用などにより、覗き見されないような対策を実施する。

⑤ 機密書類を廃棄するBOXと、保存処方箋のBOXや一般書類を廃棄するBOXとは、場所を離して設置し、紛れ込み等の誤廃棄をなくすような対策を実施する。

⑥ 電子カルテシステムのノートパソコン端末をワゴン等に乗せて使用する場合には、セキュリティワイヤの利用などの盗難対策を実施する。

⑦ 倉庫など普段職員の出入りのない場所に重要な情報資産を保管する場合には、施錠管理の他に、監視カメラやセンサーの設置などの盗難対策を実施する。

6.2 サーバ等の管理

サーバ等の機器及び通信ケーブル等の配線を所管する情報セキュリティ管理者は、以下の措置を講じる。

(1) 機器の取付け

サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、耐震対策や盗難対策など必要な措置を講じる。

(2) 機器の電源

① 当該施設の施設管理部門及び経営企画課と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付ける。

② 当該施設の施設管理部門及び経営企画課と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じる。

(3) 通信ケーブル等の配線

① 当該施設の施設管理部門及び経営企画課と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、冗長をとったり、折れ曲がりを防止したり、配線モ

ールを使用したりするなどの必要な措置を講じる。

② 主要な箇所の通信ケーブル及び電源ケーブルについては、当該施設の施設管理部門及び経営企画課から損傷等の報告があった場合、連携して対応する。

③ ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理する。

④ 自ら又は情報セキュリティ担当者、経営企画課職員及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を講じる。

(4) 機器の定期保守及び修理

① サーバ等の機器の定期保守を実施する。

② 記憶媒体を内蔵する機器を外部委託業者に修理させる場合、原則として作業を院内で行わせ、職員が立ち会う。なお、修理設備等の関係によりやむを得ない場合に限り、外部委託業者の施設で作業を行わせることができるが、この場合委託事業者との間で守秘義務契約を締結するなど秘密保持に努める。

(5) 敷地外への機器の設置

病院の敷地外にサーバ等の機器を設置する場合は、情報セキュリティ統括責任者の承認を得る。また、定期的に当該機器への情報セキュリティ対策状況について確認する。

6.3 サーバ室の管理

サーバ室を所管する情報セキュリティ管理者は、以下の措置を講じる。

(1) サーバ室の構造等

① 当該施設の施設管理部門及び経営企画課と連携して、サーバ室から外部に通じるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立ち入りを防止する。

② サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じる。

③ サーバ室に配置する消防用設備等が、機器等及び記録媒体に影響を与えないようにする。

(2) サーバ室の入退室管理等

サーバ室への入退室を許可した者のみに制限し、入退室管理対策を実施する。

(3) 機器等の搬入出

① 搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認する。

② サーバ室の機器等の搬入出について、職員を立ち会わせる。

7　人的セキュリティ

7.1 職員等の遵守事項

職員等は、以下の事項を遵守する。

(1) 情報セキュリティポリシーの遵守

情報セキュリティポリシーを遵守する。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に確認する。

(2) 情報システムの利用

① 業務目的以外で、電子カルテシステム等の情報システムを使用しない。

② 使用が終了した場合、あるいは端末を離れる場合にはログアウトを行う。

③ パスワードを十分な長さとし、ユーザID、職員番号、生年月日、名前等は使用しない。

④ パスワードは経営企画課からの周知があった場合には、速やかに変更する。

⑤ パスワードは他人には知らせない。

(3) 私物パソコン等の利用

① 私物のパソコンやモバイル端末を院内に持ち込んで業務に使用する場合には、ウイルス対策ソフトウェアをインストールし、パターンファイルを適宜更新する。

② 私物のパソコンやモバイル端末を院内の業務用インターネット回線に接続する場合には、事前に経営企画課に申請し、許可を得る。

(4) 私物記憶媒体の使用

① 私物のUSBメモリ等の記憶媒体を業務に使用する場合には、情報セキュリティ管理者の許可を得る。

② 情報セキュリティ管理者の許可を得て私物の記憶媒体を業務に使用する場合には、紛失しないよう注意するとともに、使用前後のウイルスチェックの実施、不要なファイルの削除、施錠保管を行う。

③ 記憶媒体の使用が終了した場合には、端末から取り外す。

(5) FAX送信

① 重要な情報資産を他病院等の院外にFAX送信する場合には、FAXのワンタッチボタンの使用、テスト送信の実施、複数人によるFAX番号の確認などにより誤送信を防ぐ。

② FAX送信を他の職員等に依頼する場合には、FAX番号の書き間違いや言い間違いのないよう確認する。

(6) 電子メール

① 重要な情報資産を電子メールにて送信する場合には、パスワードや暗号化などにより他人に知られないように対策を行う。

② 複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにBCCを利用して送信する。

③ 差出人が不明又は不自然なファイルの添付など、不審な電子メールを受信した場合は、添付ファイルの開封や本文内URLのクリックをせずに、経営企画課に報告し、指示を仰ぐ。

(7) 郵送

重要な情報資産を院外に郵送する場合には、複数人による宛先や封入物の確認などにより誤送付を防ぐ。

(8) 出力書類の取り出し

コピー機、ファクシミリ、プリンタ等の入出力書類を放置しない。

(9) 重要な情報資産の保管

重要な情報資産を机上、カウンター等に放置しない。

(10) 退職時等の遵守事項

異動、退職等により業務を離れる場合には、利用していた情報資産を返却する。

また、その後も業務上知り得た情報を漏らさない。

(11) 会話に関する遵守事項

① 更衣室、エスカレータ、エレベータ、ロビー等当院内の共有スペースや公共の場では患者情報など業務に関する会話をしない。

② 診療情報等に関して患者や家族と話をする場合には、個室の利用等により、第三者へ会話が聞こえないよう配慮する。

(12) インターネット閲覧及びソーシャルメディアの利用時の遵守事項

① インターネット端末では、業務目的以外でインターネットを閲覧しない。

② ソーシャルメディアを利用する場合には、磐田市立総合病院の職員であることの自覚と責任を持つとともに、「磐田市立総合病院ソーシャルメディア利用ガイドライン」に従う。

(13) 図書室のパソコン利用時の遵守事項

図書室のパソコンを利用する場合には、個人情報を取り扱わないようにし、利用終了時には、使用していたファイルを消去する。

(14) クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたっても情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識する。

7.2 情報セキュリティポリシー等の明示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシーを閲覧できるようにする。

7.3 研修・訓練

(1) 情報セキュリティに関する研修

情報セキュリティ統括責任者は、定期的に情報セキュリティに関する研修を実施する。

(2) 緊急時対応訓練

情報セキュリティ統括責任者は、緊急時対応を想定した訓練を実施する。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を定め、また、効果的に実施できるように計画する。

(3) 研修・訓練への参加

職員等は、定められた研修・訓練に参加する。

(4) 職員等への指示・周知

① 情報セキュリティ管理者は、職員等に対して、常日頃から情報セキュリティに関する啓発を実施する。

② 情報セキュリティ管理者は、情報セキュリティのヒヤリハット体験があった場合には、職員等に周知し、情報セキュリティ事故の発生防止を図る。

7.4 事故、欠陥等の報告

(1) 事故等の報告

① 職員等は、情報セキュリティに関する事故が発生した場合、情報システム上の重大な欠陥及び誤動作を発見した場合、並びに患者等外部からその旨の報告を受けた場合は、速やかに情報セキュリティ管理者に報告する。

② 報告を受けた情報セキュリティ管理者は、上長となる情報セキュリティ責任者及び経営企画課に報告する。

③ 経営企画課及び情報セキュリティ管理者は、報告のあった事故等について、必要に応じて情報セキュリティ統括責任者及び情報セキュリティ副統括責任者に報告する。

(2) 事故等の分析・記録等

事故等を引き起こした組織の情報セキュリティ管理者は、経営企画課と連携し、これらの事故等を分析し、記録を保存する。

(3) 事故等の周知、再発防止

経営企画課は、事故の分析結果について可能な範囲で院内周知を行い、再発防止を図る。

7.5 ID及びパスワード等の管理

(1) ICカード等の取扱い

① 認証に用いるICカード等を、職員等間で共有しない。

② ICカード等を紛失した場合には、速やかに情報セキュリティ管理者に報告し、指示に従う。

③ ICカード等を紛失カード等の紛失等の報告があり次第、当該ICカード等を使用したアクセスを速やかに停止する。

④ ICカード等を切り替える場合、切り替え前のカードを回収し、初期化・破砕するなど復元不可能な処理を行う。

(2) IDの取扱い

① IDを他人に利用させない。

② 共用IDを利用する場合は、関係者以外に利用させない。

(3) パスワードの取扱い

① パスワードは、他人に知られないように管理する。

② パスワードの照会等には一切応じない。

③ パスワードを十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にする。

④ パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告するとともに、パスワードを速やかに変更する。

⑤ 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

⑥ 仮のパスワード（初期パスワード含む）は、初回ログイン時に変更しなければならない。

⑦ サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

⑧ 職員等間でパスワードを共有してはならない。（ただし共用IDに対するパスワードを除く）。

8 技術的セキュリティ

8.1 コンピュータ及びネットワークの管理

(1) バックアップの実施

情報セキュリティ管理者は、バックアップについて以下の措置を講じる。

① サーバ等に記録された情報について、必要に応じて定期的にバックアップを実施する。

② 私物のUSBメモリ等の記憶媒体をバックアップとしては使用させない。

(2) システム管理記録及び作業の確認

情報システムを所管する情報セキュリティ管理者は、システム管理記録及び作業について以下の措置を講じる。

① 所管する情報システムの運用において実施した作業について、作業記録を作成する。

② 所管する情報システムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、適切に管理する。

③ 職員等及び契約により操作を認められた外部委託事業者が情報システムの変更等の作業を行う場合は2名以上で作業させ、互いにその作業を確認する。

(3) 情報システム仕様書等の管理

情報システムを所管する情報セキュリティ管理者は、ネットワーク構成図、情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりしないよう、適切に管理する。

(4) アクセス記録の取得等

情報システムを所管する情報セキュリティ管理者は、各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存するとともに、適切に管理する。

(5) 障害記録

情報システムを所管する情報セキュリティ管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存する。

(6) 通信回線及び通信回線装置の管理

通信回線等を所管する情報セキュリティ管理者は、以下の措置を講じる。

① 所管する通信回線及び通信回線装置を、当該施設の施設管理部門及び経営企画課と連携し、適切に管理する。また、通信回線及び通信回線装置に関連する文書を適切に保管する。

② 外部へのネットワーク接続を必要最小限に限定する。

③ 情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択する。また、必要に応じ、送受信される情報の暗号化等の情報漏えい防止策を講じる。

(7) スクリーンセーバの設定

情報システムを所管する情報セキュリティ管理者は、必要により、スクリーンセーバにパスワードを設定する。

(8) 無線LAN 及びネットワークの盗聴対策

無線LANを利用する場合、ネットワークを所管する情報セキュリティ管理者の許可を得て、解読が困難な暗号化及び認証技術を使用する。

(9) 電子メールのセキュリティ管理

電子メールサーバを所管する情報セキュリティ管理者は、電子メールのセキュリティ管理について以下の措置を講じる。

① 権限のない利用者により、外部から外部への電子メール転送（電子メールの中継

処理）が行われることを不可能とするよう、電子メールサーバの設定を実施する。
② 大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止する。
③ 電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にする。
④ 職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知する。
⑤職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように、添付ファイルの監視等によるシステム上の措置をする。
⑥ 職員等は、重要な情報資産を外部に送信する場合には、電子署名、暗号化又はパスワード設定の方法を使用して送信する。

(10) ソフトウェアの導入制限

職員等は、インターネットパソコン等にソフトウェアを無断で導入してはならない。ただし、業務上必要なソフトウェアを導入する場合には、情報セキュリティ管理者の許可を得て、経営企画課に導入を依頼する。

(11) 機器構成の変更制限

職員等は、インターネットパソコン等の機器構成を無断で変更してはならない。ただし、業務上必要な改造及び増設・交換を行う場合には、情報セキュリティ管理者の許可を得て、経営企画課に変更を依頼する。

(12) ネットワークの接続制限

職員等は、パソコン等をネットワークに無断で接続してはならない。ただし、業務上必要な場合には、情報セキュリティ管理者の許可を得て、経営企画課に実施を依頼する。

(13) インターネットの閲覧

① 情報セキュリティ統括責任者は、職員等のインターネット利用について、明らかに業務に関係のないインターネットを閲覧していた場合は、当該職員等が所属する情報セキュリティ管理者に通知し適切な措置を求める。
② 職員等は、契約行為が発生しないオンラインストレージサービスにて個人情報を含むファイルを扱ってはならない。

(14) Web会議サービスの利用

① Web会議を開催する場合は、原則として自組織から支給された端末を利用する。ただし視聴や参加の際の端末についてはこの限りでない。
② 利用するWeb会議サービスのソフトウェアが、最新の状態であることを確認する。
③ 重要な情報資産を取り扱う場合は、可能な限りエンドツーエンド（E2E）の暗号化を行う。
④ 重要な情報資産を取り扱う場合は、Web会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、E2Eの暗号化を利用できなくなる機能を可能な限り使用しない。
⑤ 音声を扱う場合は、ヘッドホンを利用する、個室を利用するなど、内容が周囲に漏れないよう注意する。
⑥ Web会議にアクセスするためのパスワードを設定する。

(15) ソーシャルメディアサービスの利用

① 職員等は、「磐田市立総合病院ソーシャルメディア利用ガイドライン」に則り適切に利用する。

8.2 アクセス制御

(1) アクセス制御

ネットワーク及び情報システムを所管する情報セキュリティ管理者は、アクセスする権限のない職員等がアクセスできないように、システム上制限する。

(2) 利用者IDの取り扱い

ネットワーク及び情報システムを所管する情報セキュリティ管理者は、利用者IDの取り扱いについて以下のとおりとする。

① 利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者IDの取り扱い等を適正に管理する。

② 利用されていないIDが放置されないよう、人事管理部門と連携し、点検する。

(3) 特権を付与されたIDの管理等

ネットワーク及び情報システムを所管する情報セキュリティ管理者は、管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理する。

(4) パスワードに関する情報の管理

ネットワーク及び情報システムを所管する情報セキュリティ管理者は、パスワードに関する情報の管理について以下の措置を講じる。

① 職員等のパスワードに関する情報を厳重に管理する。

② 職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させる。

③ 必要により、定期的にパスワードの変更を行うよう職員等に周知する。

(5) 職員等による外部からのアクセス等の制限

① 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、ネットワーク及び情報システムを所管する情報セキュリティ管理者の許可を得る。

② ネットワーク及び情報システムを所管する情報セキュリティ管理者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを許可する場合は、利用者のID、パスワード及び生体認証に係る情報等の認証情報またはICカード等による認証に加えて、通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じる。

③ ネットワーク及び情報システムを所管する情報セキュリティ管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定する。

④ ネットワーク及び情報システムを所管する情報セキュリティ管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保する。

⑤ ネットワーク及び情報システムを所管する情報セキュリティ管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じる。

(6) ログイン時の表示等

① 情報システムを所管する情報セキュリティ管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを

確認することができるようシステムを設定する。

(7) 認証情報の管理

① 情報システムを所管する情報セキュリティ管理者は、職員等の認証情報を厳重に管理する。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用する。

② 情報システムを所管する情報セキュリティ管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させる。

③ 情報システムを所管する情報セキュリティ管理者は、認証情報の不正利用を防止するための措置を講じる。

(8) 特権による接続時間の制限

情報システムを所管する情報セキュリティ管理者は、特権による情報システムへの接続時間を必要最小限に制限する。

8.3 システム開発、導入、保守等

情報システムを所管する情報セキュリティ管理者は、情報システムの開発、導入、保守等について以下のとおりとする。

(1) 情報システムの調達

① 情報システムの開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記する。

② 機器及びソフトウェアの調達に当たり、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認する。

(2) 情報システムの開発

① 情報システムの開発責任者及び作業者を特定する。

② システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、開発用IDを削除する。

③ システム開発の責任者及び作業者が使用するハードウエア及びソフトウェアを特定する。

(3) 情報システムの導入

① システム開発、保守及びテスト環境とシステム運用環境を分離する。

② 新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分なテストを実施する。

③ 個人情報及び機密性の高い生データを、テストデータに使用してはならない。

(4) システム開発・保守に関連する資料等の保管

システム開発・保守に関連する資料及び文書を適切な方法で保管する。

(5) 情報システムにおける入出力データの正確性の確保

① 情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計する。

② 情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計する。

(6) 情報システムの仕様変更管理

情報システムの仕様を変更する場合、プログラム仕様書等の変更履歴を作成する。

(7) 開発・保守用のソフトウェアの更新等

開発・保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性を確認する。

(8) システム更新又は統合時の検証等

システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行う。

8.4 不正プログラム対策

(1) 情報セキュリティ統括責任者の措置事項

情報セキュリティ統括責任者は、不正プログラム対策について以下の措置を講じる。

① 外部ネットワークから受信したファイルを、インターネットのゲートウェイにおいて不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止させる。

② 外部ネットワークに送信するファイルを、インターネットのゲートウェイにおいて不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止させる。

③ 不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起する。

(2) 情報セキュリティ管理者の措置事項

情報セキュリティ管理者は、不正プログラム対策について以下のとおり措置を講じる。

① 所管するサーバ及びパソコン等に、不正プログラム対策ソフトウェアを常駐させる。

②不正プログラム対策ソフトウェア及びパターンファイルを常に最新の状態に保つ。

③ パソコン等に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施する。

④ ネットワークに接続していないシステムにおいても、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施する。

⑤ 不正プログラムの被害を防止するため、業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したものを利用しない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認する。

(3) 職員等の遵守事項

職員等は、不正プログラム対策について以下の事項を遵守する。

① 不正プログラム対策ソフトウェアの設定を変更してはならない。

② 外部からデータ等を取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを実施する。

③ 経営企画課が提供する不正プログラム情報を常に確認する。

④ 不正プログラムを検出した場合には、LAN ケーブルを即時取り外し、情報セキュリティ管理者及び経営企画課に連絡する。

8.5 不正アクセス対策

(1) 情報セキュリティ統括責任者の措置事項

情報セキュリティ統括責任者は、以下の措置を講じる。

① 使用されていないポートを閉鎖する。

② 不要なサービスについて、機能を削除又は停止する。

③ 情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築する。

(2) 攻撃への対処

① サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じる。また、関係機関と連絡を密にして情報の収集に努める。

(3) 記録の保存

① サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努める。

(4) 内部からの攻撃

① 情報システムを所管する情報セキュリティ管理者は、職員等及び外部委託事業者が使用しているパソコン等からの不正アクセス、院内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視する。

(5) 職員等による不正アクセス

① 情報セキュリティ統括責任者は、職員等による不正アクセスがあった場合は、当該職員等が所属する情報セキュリティ管理者に通知し適切な措置を求める。

(6) ネットワークの接続制御、経路制御等

ネットワークを所管する情報セキュリティ管理者は、ネットワークの接続制御及び経路制御等について以下のとおりとする。

① フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定する。

② 不正アクセスを防止するため、ネットワークに適切なアクセス制御を実施する。

(7) 外部ネットワークとの接続制限等

ネットワーク及びインターネット公開サーバ等を所管する情報セキュリティ管理者は、外部ネットワークとの接続制御等について以下のとおりとする。

① 外部ネットワークと接続しようとする場合は、情報セキュリティ統括責任者の許可を得る。

② 経営企画課と連携して、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、院内のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認する。

③ 接続した外部ネットワークの瑕疵(かし)によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保する。

④ 院内ネットワークへの侵入を防御するために、経営企画課と連携してファイアウォール等を外部ネットワークとの境界に設置した上で接続する。

⑤ 接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、情報セキュリティ統括責任者の判断に従い、速

やかに当該外部ネットワークを物理的に遮断する。

(8) サービス不能攻撃

情報セキュリティ統括責任者及び情報システムを管轄する情報セキュリティ管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じる。

(9) 標的型攻撃

情報セキュリティ統括責任者及び情報システムを管轄する情報セキュリティ管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じる。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検視して対処する対策（内部対策及び出口対策）を講じる。

8.6 セキュリティ情報の収集

ネットワーク及び情報システムを所管する情報セキュリティ管理者は、セキュリティ情報の収集について以下のとおりとする。

(1) セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じて関係者間で共有する。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施する。

(2) 不正プログラム等のセキュリティ情報の収集・周知

不正プログラム等のセキュリティ情報を収集し、必要に応じて対応方法を職員等に周知する。

(3) 情報セキュリティに関する情報の収集及び共有

情報セキュリティ統括責任者及び情報システムを管轄する情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有する。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じる。

9 運用

9.1 情報システムの監視

情報システムを所管する情報セキュリティ管理者は、情報システムの監視について以下の措置を講じる。

① 情報セキュリティに関する事案を検知するため、情報システム及び外部と常時接続するシステムを常時監視する。

② 重要なアクセスログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じる。

③ 外部と常時接続するシステムを常時監視する。

9.2 情報セキュリティポリシーの遵守状況の確認

(1) 遵守状況の確認及び対処

① 情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について監査や自己点検などで確認を行い、問題を認めた場合には、速やかに情報セキュリティ統括責任者及び情報セキュリティ副統括責任者に報告する。

② 情報セキュリティ統括責任者は、発生した問題について、適切かつ速やかに対処する。

③ ネットワーク及び情報システムを所管する情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処する。

(2) パソコン等及び記録媒体等の利用状況調査

情報セキュリティ統括責任者は、不正利用、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン等及び記録媒体のアクセス記録、インターネットの閲覧、電子メールの送受信記録等の利用状況を調査させることができる。

(3) 職員等の報告義務

職員等は、情報セキュリティポリシーに対する違反行為を行うか、発見した場合には、直ちに情報セキュリティ管理者に報告する。

9.3 侵害時の対応等

(1) 緊急時対応計画の策定

① 情報セキュリティ統括責任者及び情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処する。

② 情報セキュリティ統括責任者又は情報セキュリティ委員会は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処する。

(2) 緊急時対応計画に盛り込むべき内容

① 関係者の連絡先

② 発生した事案に係る報告すべき事項

③ 発生した事案への対応措置

④ 再発防止措置の策定

(3) 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保する。

(4) 緊急時対応計画の見直し

情報セキュリティ統括責任者又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直す。

（１０ 業務委託と外部サービスの利用へ移動）

9.4 例外措置

(1) 例外措置の許可

情報セキュリティ管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、業務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、情報セキュリティ統括責任者の許可を得て、例外措置を取る。

(2) 緊急時の例外措置

情報セキュリティ管理者は、業務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに情報セキュリティ統括責任者に報告する。

(3) 例外措置の記録

情報セキュリティ統括責任者は、例外措置の記録を適切に保管する。

9.5 法令等の遵守

(1) 職員等は、職務の遂行において使用する情報資産を保護するために、次の法令や規程類のほか関係法令を遵守し、これに従う。

① 地方公務員法(昭和二十五年十二月十三日法律第二百六十一号)
② 著作権法（昭和四十五年法律第四十八号）
③ 不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）
④ 磐田市電子計算組織の運営及びデータ保護に関する規程（平成十七年四月一日訓令第八号）
⑤ 磐田市情報公開条例（平成十七年四月一日条例第二十五号）
⑥ 個人情報の保護に関する法律（平成十五年法律第五十七号 令和五年法律第七十九号による改正）
⑦ 磐田市立総合病院個人情報保護方針
⑧ 磐田市立総合病院個人情報保護規程
⑨ 磐田市立総合病院医療情報システム運用管理規程（平成26年4月1日改定）
⑩ 厚生労働省　医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン
⑪ サイバーセキュリティ基本法（平成二十八年法律第三十一号）

(2) ネットワーク及び情報システムを所管する情報セキュリティ管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従う。

9.6 懲戒処分等

(1) 懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、懲戒規程及び地方公務員法による懲戒処分の対象とする。

(2) 違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに

次の措置を講じる。

① 情報セキュリティ統括責任者は、当該職員等が所属する部、科、課、室等の情報セキュリティ管理者に通知し、適切な措置を求める。

② 当該職員等が所属する科、課、室等の情報セキュリティ管理者は、経営企画課と協力して適切な措置を講じる。

③ 情報セキュリティ統括責任者は、情報セキュリティ管理者の指導によっても改善されない場合には、当該職員等の情報システムの利用を停止させる。

１０ 業務委託と外部サービスの利用

10.1 外部委託

ネットワーク及び情報システムを所管する情報セキュリティ管理者は、外部委託について以下のとおりとする。

(1) 外部委託先の選定基準

外部委託先の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認する。必要に応じてISMSやITSMS、プライバシーマーク等の公的認証を取得している事業者を選定する。

(2) 契約項目

ネットワーク及び情報システムの開発、導入、保守、運用等を外部委託する場合には、委託事業者との間で必要に応じて以下の情報セキュリティ要件を明記した契約を締結する。

① 業務上知り得た情報の守秘義務（委託業務終了後も含む）

② 提供された情報の返還義務（複写の禁止）

③ 当院に対する報告義務（個人情報の取り扱い等の有無）

④ 当院による監査、検査の実施権限

⑤ 情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

⑥ 再委託に関する制限事項の遵守

(3) 確認・措置等

外部委託事業者において必要な情報セキュリティ対策が確保されていることを定期的に確認し、必要に応じ(2)契約項目に基づき措置する。また、その内容を情報セキュリティ責任者に報告するとともに、その重要度に応じて情報セキュリティ統括責任者に報告する。

10.2 外部サービスの利用（「重要な情報資産」の情報を取り扱う場合）

(1) 外部サービスの利用に係る規定の整備

情報セキュリティ統括責任者は、以下を含む外部サービスの利用に関する規定（「重要な情報資産」の情報を取り扱う場合）を整備する。

① 外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下10.2節において「外部サービス利用判断基準」と

いう。）
② 外部サービス提供者の選定基準
③ 外部サービス利用申請の許可権限者と利用手続
④ 外部サービス管理者の指名と外部サービスの利用状況の管理

(2) 外部サービスの選定
① 情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討する。
② 情報セキュリティ管理者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定する。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含める。
（ア）外部サービスにおいて医療情報を扱う場合には、総務省・経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」及び厚生労働省「医療情報システムの安全管理に関するガイドライン」を遵守すること
（イ）外部サービスの利用を通じて当院が取り扱う情報の外部サービス提供者における目的外利用の禁止
（ウ）外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制
（エ）外部サービスの提供に当たり、提供者若しくはその従業員、再委託先又はその他の者によって、当院の意図しない変更が加えられないための管理体制
（オ）外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定
（カ）情報セキュリティインシデントへの対処方法
（キ）情報セキュリティ対策その他の契約の履行状況の確認方法
（ク）情報セキュリティ対策の履行が不十分な場合の対処方法
③ 情報セキュリティ管理者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含める。
④ 情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認する。
⑤ 情報セキュリティ管理者は、外部サービスの利用を通じて当院が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含める。
（注）クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定める。クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が当院によって受容可能か判断すること。
（ア）情報セキュリティ監査の受入れ
（イ）サービスレベルの保証
⑥ 情報セキュリティ管理者は、外部サービスの利用を通じて当院が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供

者を選定し、必要に応じて当院の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含める。

⑦ 情報セキュリティ管理者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を当院に提供し、当院の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断する。

⑧ 情報セキュリティ管理者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定める。

⑨ 情報セキュリティ統括責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断する。

(3) 外部サービスの利用に係る調達・契約

① 情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含める。

② 情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含める。

(5) 外部サービスの利用承認

① 情報セキュリティ管理者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行う。

② 利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定する。

③ 利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、情報セキュリティ管理者を外部サービス管理者として指名し、承認済み外部サービスとして記録する。

(6) 外部サービスを利用した情報システムの導入・構築時の対策

① 情報セキュリティ統括責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定する。

（ア）不正なアクセスを防止するためのアクセス制御

（イ）取り扱う情報の機密性保護のための暗号化

（ウ）開発時におけるセキュリティ対策

（エ）設計・設定時の誤りの防止

（オ）クラウドサービスにおけるユーティリティプログラムに対するセキュリティ

対策

② 情報セキュリティ管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録する。

③ 情報セキュリティ管理者は、前各項において定める規定に対し、情報セキュリティに配慮した構築の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を確認及び記録する。

(7) 外部サービスを利用した情報システムの運用・保守時の対策

① 情報セキュリティ統括責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定する。

（ア）外部サービス利用方針の規定
（イ）外部サービス利用に必要な教育
（ウ）取り扱う資産の管理
（エ）不正アクセスを防止するためのアクセス制御
（オ）取り扱う情報の機密性保護のための暗号化
（カ）外部サービス内の通信の制御
（キ）設計・設定時の誤りの防止
（ク）外部サービスを利用した情報システムの事業継続
（ケ）設計・設定変更時の情報や変更履歴の管理

② 情報セキュリティ管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備する。

③ 情報セキュリティ管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録する。

④ 情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録する。

(8) 外部サービスを利用した情報システムの更改・廃棄時の対策

① 情報セキュリティ統括責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定する。

（ア）外部サービスの利用終了時における対策
（イ）外部サービスで取り扱った情報の廃棄
（ウ）外部サービスの利用のために作成したアカウントの廃棄

② 情報セキュリティ管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録する。

② 情報セキュリティ管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態とする。

10.3 外部サービスの利用（「重要な情報資産」の情報を取り扱わない場合）

(1) 外部サービスの利用に係る規定の整備

情報セキュリティ統括責任者は、以下を含む重要な情報資産を取り扱わない場合の外部サービス利用規定（以下10.3節において「外部サービス利用規程」という。）を整備する。

① 外部サービスを利用可能な業務の範囲
② 外部サービス利用申請の許可権限者と利用手続
③ 外部サービス管理者の指名と外部サービスの利用状況の管理
④ 外部サービス利用の運用手順

(2) 外部サービスの利用検討

① 職員等は所属部署の情報セキュリティ管理者に対し、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で「重要な情報資産」の情報を取り扱わない場合の外部サービスの利用を申請する。

② 情報セキュリティ管理者は、外部サービス利用規定に従い、職員等による外部サービスの利用申請を審査し、利用の可否を決定する。

１１ 評価・見直し

11.1 情報セキュリティ監査

(1) 実施方法

情報セキュリティ副統括責任者は、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的に又は必要に応じて情報セキュリティ監査を実施する。

(2) 情報セキュリティ監査を行う者の要件

① 被監査部門から独立した者。
② 情報セキュリティ監査及び情報セキュリティに関する専門知識を有する者。

(3) 情報セキュリティ監査実施計画の立案及び実施への協力

① 情報セキュリティ副統括責任者は、情報セキュリティ監査実施計画を立案し、情報セキュリティ委員会の承認を得る。
② 被監査部門は、情報セキュリティ監査の実施に協力する。

(4) 外部委託事業者に対する情報セキュリティ監査

① 情報資産に関する業務を外部委託事業者に委託している場合、情報セキュリティ副統括責任者は情報セキュリティポリシーの遵守について、情報セキュリティ監査を定期的に又は必要に応じて実施する。
② クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行う。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

(5) 報告

情報セキュリティ副統括責任者は、情報セキュリティ監査結果を取りまとめ、情報セキュリティ委員会に報告する。

(6) 保管

情報セキュリティ副統括責任者は、情報セキュリティ監査の実施を通して収集した証拠書類、情報セキュリティ監査報告書の作成のための調書を、紛失等が発生しないように適切に保管する。

(7) 情報セキュリティ監査結果への対応

情報セキュリティ統括責任者は、情報セキュリティ監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示する。さらに他の情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させる。

(8) 情報セキュリティポリシーの見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用する。

11.2 自己点検

(1) 実施方法

① 情報セキュリティ管理者は、所管する部、科、課、室等における情報セキュリティ対策状況について、毎年度又は必要に応じ自己点検を実施し、結果及び改善策案を情報セキュリティ責任者及び経営企画課に報告する。

② ネットワーク及び情報システムを所管する情報セキュリティ管理者は、所管するネットワーク及び情報システムについて、定期的に又は必要に応じ自己点検を実施し、結果及び改善策案を情報セキュリティ責任者及び経営企画課に報告する。

(2) 報告

情報セキュリティ責任者及び経営企画課は、報告された自己点検結果とそれに基づく改善策を取りまとめ、情報セキュリティ委員会に報告する。

(3) 自己点検結果の活用

① 情報セキュリティ管理者は、自己点検の結果に基づき、自己の権限の範囲内で改善を図る。

② 情報セキュリティ委員会は、自己点検結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用する。

11.3 情報セキュリティポリシーの見直し

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果や情報セキュリティに関する状況の変化により、新たに対策が必要になった場合には、情報セキュリティポリシーの見直しを実施する。